

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-070566

(43)Date of publication of application : 10.03.1998

(51)Int.Cl.

H04L 12/46

H04L 12/28

H04L 12/66

H04L 29/08

(21)Application number : 08-227970

(71)Applicant : KOKUSAI DENSHIN DENWA CO LTD <KDD>

(22)Date of filing : 29.08.1996

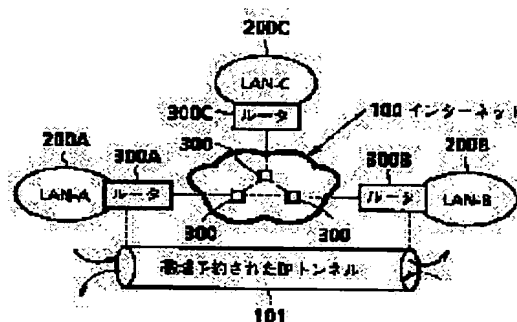
(72)Inventor : MAEJIMA OSAMU
ITO YOSHIHIRO
ISHIKURA MASAMI
ASAMI TORU

(54) BAND SECURING TYPE VPN CONSTRUCTING METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To secure VPN(virtual private network) by the unit of a host or a sub-net.

SOLUTION: An IP tunnel 101 is constituted between routers 300A and 300B connected to internet 100 and a network resource reserving type protocol is started on this IP tunnel 101 to reserve the transmitting band width of the IP tunnel 101 to secure the band of VPN by the unit of the host to the sub-net. In addition, as the traffic control of routers 300A, 300 and 300B on the IP tunnel 101, the sending frequency of a packet which an inputting processor and an outputting processor within each router process is assigned by the ratio of a transmission band width reserved to the IP tunnel to simplify the algorithm of traffic control. In addition, each router 300A, 300 and 300B on the IP tunnel is provided with a reserving schedule function to manage the using time of band securing type VPN to secure a band at a designation date.



LEGAL STATUS

[Date of request for examination]

06.02.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

3591996

[Date of registration]

03.09.2004

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平 10 - 70566

(43) 公開日 平成 10 年 (1998) 3 月 10 日

(51) Int. Cl. ⁸	識別記号	庁内整理番号	F I	技術表示箇所
H04L 12/46			H04L 11/00	310 C
12/28		9744-5K	11/20	B
12/66			13/00	307 Z
29/08				

審査請求 未請求 請求項の数 3 O L (全 9 頁)

(21) 出願番号 特願平 8 - 227970

(22) 出願日 平成 8 年 (1996) 8 月 29 日

(71) 出願人 000001214

国際電信電話株式会社

東京都新宿区西新宿 2 丁目 3 番 2 号

(72) 発明者 前島 治

東京都新宿区西新宿 2 丁目 3 番 2 号 国際
電信電話株式会社内

(72) 発明者 伊藤 嘉浩

東京都新宿区西新宿 2 丁目 3 番 2 号 国際
電信電話株式会社内

(72) 発明者 石倉 雅巳

東京都新宿区西新宿 2 丁目 3 番 2 号 国際
電信電話株式会社内

(74) 代理人 弁理士 光石 俊郎 (外 2 名)

最終頁に続く

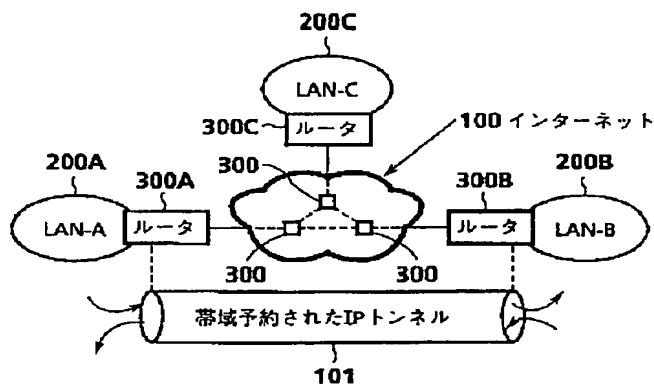
(54) 【発明の名称】 帯域確保型 V P N 構築方法

(57) 【要約】

【課題】 V P N の帯域をホスト或いはサブネット単位で確保すること。

【解決手段】 インターネット 100 に接続されるルータ 300 A、300 B 間に I P トンネル 101 を構成し、この I P トンネル 101 上に網資源予約型プロトコルを起動させて同 I P トンネル 101 の伝送帯域幅を予約することにより、ホスト或いはサブネット単位で V P N の帯域確保を行う。また、I P トンネル 101 上のルータ 300 A、300、300 B のトラヒック制御として、各ルータ内部の入力プロセッサ及び出力プロセッサが処理するパケットの送出頻度を、I P トンネルに予約した伝送帯域幅の比で割り当てることにより、トラヒック制御のアルゴリズムを簡素化する。更に、I P トンネル 101 上の各ルータ 300 A、300、300 B に予約スケジュール機能を持たせ、帯域確保型 V P N の使用時間の管理を行うことにより、指定した日時での帯域確保を可能とする。

ネットワークモデル (実施例)



【特許請求の範囲】

【請求項 1】 インターネットに接続されるルータ間に I P トンネルを構成し、この I P トンネル上に網資源予約型プロトコルを起動させることにより同 I P トンネルの伝送帯域幅の予約を行うことを特徴とする帯域確保型 V P N 構築方法。

【請求項 2】 I P トンネル上のルータのトラヒック制御として、同ルータ内部の入力プロセッサ及び出力プロセッサが処理するパケットの送出頻度を、各 I P トンネルに予約した伝送帯域幅の比で割り当てることを特徴とする請求項 1 に記載の帯域確保型 V P N 構築方法。

【請求項 3】 I P トンネル上の各ルータに予約スケジュール機能を持たせ、帯域確保型 V P N の使用時間の管理を行うことを特徴とする請求項 1 または 2 に記載の帯域確保型 V P N 構築方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明はインターネット (Internet) 上に V P N (Virtual Private Network (パチャルプライベートネットワーク：仮想的専用網) の略記表示) を構築する方法に関し、特に、所望の伝送帯域幅の予約或いは確保をホスト単位或いはサブネット単位で可能にするものである。

【0002】

【従来の技術】 V P N とは、インターネット等の公衆網上で論理的なグループを構成し、且つ、そのグループ間で閉域性を保つ仕組みを設けたネットワークのことである。

【0003】 インターネット等の公衆網には、通常、不特定多数のユーザが接続している。そのため、基本的には特定のユーザだけの通信は出来ず、第三者による不正なアクセスが避けられないといったセキュリティ上の問題がある。

【0004】 そこで、近年、End-End (エンドーエンド) でセキュリティ対策を施すことによりインターネット上に仮想的に専用線を構築し、L A N (Local Area Network の略記表示) 間接続の基幹回線として利用する V P N 技術が注目されている。

【0005】 具体的には、従来の V P N では、エンドーエンドでのデータの暗号化、ユーザ認証及びアクセス制御等のセキュリティを施した上で、特定の拠点間をインターネットを介して接続し、閉域性の有るグループを提供している。

【0006】 このような V P N を公衆網上に実現することにより、特定のユーザだけの通信が可能になり、インターネット等を仮想的な専用網として利用することができる。しかし、従来の V P N はその仕様上、帯域等の網資源 (ネットワークリソース) を保証していない。

【0007】 つまり、従来の V P N は本来の専用線とは異なり、他のトラヒックの影響を受けて帯域幅が変動す

るため、通信特性を予測し難いといった問題がある。

【0008】 一方、QoS (Quality of Service の略記表示：帯域、遅延、揺らぎ等のサービス品質のこと) を重視した網資源予約型プロトコルである R S V P (Resource Reservation Protocol の略記) が提案されている。

【0009】 具体的には、図 7 に示すように、インターネット 100 に接続される特定の L A N 200 A と 200 B のホスト (端末) 201 全て、並びに、L A N 200 A と 200 B 間のルータ 300 A、300 及び 300 B 全てに、アプリケーション単位で R S V P をサポートさせている。図 7 中、記号 R は R S V P のサポートを表す。

【0010】 そして、個々のアプリケーション毎に R S V P により、特定のサービス品質を満たす網資源、例えば特定の帯域幅をネットワークに要求して予約し確保する。つまり従来は、エンドーエンドで、R S V P によりアプリケーション単位に網資源を予約している。

【0011】 因みに、図 8 に示すように、ルータ 300 A、300 及び 300 B だけにアプリケーション単位で R S V P をサポートさせたとしても、両端のルータ 300 A と 300 B で終端されてしまうため、R S V P 上のアプリケーション 202 は双方の L A N 200 A、200 B へは接続されない。

【0012】 さて、従来の V P N に R S V P を組み合わせれば V P N の帯域を確保できるようにも思えるが、実際には、下記 (1)、(2) の問題がある。

(1) 従来は、R S V P によりエンドーエンドで網資源 (例えば帯域) を確保するので、V P N に接続した既存の全てのホストが R S V P をサポートしなければならない。

(2) 現在の V P N 利用方法の観点から見るとアプリケーション単位よりもホスト単位、サブネット単位の管理が望まれる場合も多く、そのような場合には、従来のアプリケーション単位での帯域確保は適さない。なお、サブネットとは、I P アドレスのホスト部を更に分割 (ネットワーク部とホスト部) して作成されたネットワークであり、図 7 や図 8 中でいえば L A N 200 A、200 B を細分化したネットワークである。

【0013】

【発明が解決しようとする課題】 本発明は、上記問題点に鑑み、ホスト単位或いはサブネット単位で伝送帯域幅を確保することができる帯域確保型 V P N を構築する方法を提供することを目的とする。

【0014】

【課題を解決するための手段】 上記課題を解決するため、本発明の帯域確保型 V P N 構築方法は、インターネットに接続されるルータ間に I P トンネルを構成し、この I P トンネル上に網資源予約型プロトコルを起動させることにより同 I P トンネルの伝送帯域幅の予約を行うことを特徴とする。

【 0 0 1 5 】 また、本発明の帯域確保型 V P N 構築方法は、上記に加えて、 I P トンネル上のルータのトラヒック制御として、同ルータ内部の入力プロセッサ及び出力プロセッサが処理するパケットの送出頻度を、各 I P トンネルに予約した伝送帯域幅の比で割り当てることを特徴とする。

【 0 0 1 6 】 更に、本発明の他の帯域確保型 V P N 構築方法は、上記に加えて、 I P トンネル上の各ルータに予約スケジュール機能を持たせ、帯域確保型 V P N の使用時間の管理を行うことを特徴とする。

【 0 0 1 7 】

【 発明の実施の形態 】

（発明の原理）次に、図 9 （ a ）（ b ）と図 1 0 を参照して、本発明に係る帯域確保型 V P N 構築方法の原理を説明する。

【 0 0 1 8 】 図 9 （ a ）に示す例では、インターネット 1 0 0 に接続されるルータ 3 0 0 A と 3 0 0 B 間に I P トンネル 1 0 1 を構成する。ここで、 I P とはインターネットプロトコル（ Internet Protocol ）の略記表示である。また、 I P トンネル 1 0 1 とは、周知の如く、ルータ 3 0 0 A と 3 0 0 B （ I P トンネル 1 0 1 の始点と終点）の I P アドレス等が記述された I P ヘッダを元のパケットに付加（カプセル化）することによって構成されるパケットが存在する区間である。終点のルータ例えば 3 0 0 B では逆に、付加された I P ヘッダを外す。

【 0 0 1 9 】 従って、両端のルータ 3 0 0 A と 3 0 0 B がそれぞれ属するネットワーク（図 9 では L A N ） 2 0 0 A 、 2 0 0 B 間のトラヒックを全て I P トンネル 1 0 1 に通すことにより、 I P トンネル 1 0 1 が L A N 2 0 0 A 及び 2 0 0 B にとっての V P N となる。

【 0 0 2 0 】 このような I P トンネル 1 0 1 上の各ルータ 3 0 0 A 、 3 0 0 及び 3 0 0 B に R S V P （網資源予約型プロトコル）をサポートさせ、 I P トンネル 1 0 1 上に R S V P を起動させる。この結果、 R S V P による帯域確保は I P トンネル 1 0 1 即ちルータ間にて行われるため、双方の L A N 2 0 0 A 、 2 0 0 B 上のアプリケーション 2 0 2 は I P トンネルの始点にてカプセル化され、ルータ 3 0 0 A ～ 3 0 0 B 間で R S V P 対応アプリケーションのデータとして I P トンネル 1 0 1 上に確保された網資源（例えば帯域）を利用することが可能である。ここで、図 9 （ b ）に示すように、 I P トンネル 1 0 1 区間は R S V P の帯域確保区間（本例ではルータ 3 0 0 A ～ 3 0 0 B 間） 1 0 2 を含む範囲にあれば良い。つまり、 I P トンネル 1 0 1 毎に伝送帯域幅の予約を行うことができる。また、伝送帯域幅の予約は従来のアプリケーション単位ではなく、各 L A N 2 0 0 A と 2 0 0 B 上の各ホスト単位或いはサブネット単位で行われる。更に、各ホスト 2 0 1 は R S V P をサポートする必要がなくなる。

【 0 0 2 1 】 また、伝送帯域幅の予約を解除するには、

I P トンネル 1 0 1 の一端のルータ 3 0 0 A （または 3 0 0 B ）から他のルータ 3 0 0 及び 3 0 0 B （または 3 0 0 及び 3 0 0 A ）に対して、 R S V P プロトコルにより解除メッセージを送信すれば良い。

【 0 0 2 2 】 このように、 R S V P プロトコル上で伝送帯域幅の確保が行われることから、各ノードのパラメータを手作業で変更する必要がなく、人的コストを削減でき、短期的な帯域需要に対して迅速且つ柔軟に帯域幅を割り当てることが可能である。また、帯域確保の解除も容易である。

【 0 0 2 3 】 以上のように、 I P トンネル 1 0 1 と網資源予約型プロトコル（ R S V P ）を組み合わせることにより、他のトラヒックの影響を受けず、ホスト 2 0 1 単位またはサブネット単位の帯域確保が可能な V P N を構築することができる。

【 0 0 2 4 】 ところで、 R S V P は網資源の予約や確立を行うプロトコルであるが、ルータやホストにおける Q o S （帯域、遅延、揺らぎ等）を保証するための具体的な制御方法については、何も規定していない。従って、ネットワークにおける Q o S 保証はルータやスイッチのトラヒック制御の実装に大きく依存する。パケットやスケジューリングのアルゴリズムとして報告されている W F Q （ Weighted Fair Queueing ）等は、アプリケーションのトラヒック特性に応じて優先度を決定し帯域や遅延特性を制御するものであり、複雑なアルゴリズムである。

【 0 0 2 5 】 本例では、 I P トンネル 1 0 1 毎に網資源パラメータとして伝送帯域幅のみを予約するので、帯域保証のための制御は、上記複雑なアルゴリズムではなく、図 1 0 に示すような単純なパケットスケジューリングのアルゴリズムで対応可能である。特に、各ルータ 3 0 0 A 、 3 0 0 、 3 0 0 B 内部の入力プロセッサ及び出力プロセッサによって処理されるパケット数を、各 I P トンネル 1 0 1 に予約した伝送帯域幅の比で割り当てるというアルゴリズムを用いることにより、 I P トンネル 1 0 1 上の各ルータ 3 0 0 A 、 3 0 0 、 3 0 0 B のトラヒック制御が極めて簡素化する。

【 0 0 2 6 】 図 1 0 の場合は、パケットスケジューラ 4 0 1 と、 # 1 から # n の複数の R S V P 用（ I P トンネル用）バッファ 4 0 2 と、非 R S V P 用バッファ 4 0 3 とでパケットスケジューリングを行う。即ち、隣接する任意のルータ間の帯域は複数の I P トンネルの分とそれ以外（非 I P トンネル）の分に区分されるので、ルータ内のバッファスペースも同様に、複数の R S V P 用バッファ 4 0 2 と、非 R S V P 用バッファ 4 0 3 に分ける。 I P トンネル内ではアプリケーションを特定する必要がないため、各 R S V P 用バッファ 4 0 2 に到着するパケットは同じトラヒック特性分布を有すると仮定する。そして、各 R S V P 用バッファ 4 0 2 のバッファサイズ及びパケットスケジューラ 4 0 1 による各 R S V P 用バッファ 4 0 2 からのパケット送出頻度を、各 I P トンネル

に予約した伝送帯域幅の比によって振り分けることで、アルゴリズムを簡素化する。

【0027】なお、非RSVP用バッファ403からのパケット送出は、RSVP用バッファ402にパケットが無い場合に行う等、優先度を低くする。

【0028】更に、本来RSVPを用いた網資源の予約では、網資源を必要とする時にしか予約を行わないものである。しかし、IPトンネル101上の各ルータ300A、300B、300Cに予約スケジュール機能を持たせて帯域確保型VPNの使用時間の管理を行うことにより、従来のRSVPを拡張し、日時を指定して伝送帯域幅を予約することができる。

【0029】（実施例）次に、図1～図6を参照して、本発明の実施例を説明する。図1は本発明を適用したネットワークモデルを示す。図2はルータ内部のトラヒック制御の構成例を示し、図3は図2の構成におけるトラヒック制御手順を示す。図4はトラヒック制御におけるパケットキューイングの説明図である。図5と図6はルータにおけるVPN予約スケジュールの処理手順（その1、その2）を示す。

【0030】図1のネットワークモデルでは、インターネット100に3個のLAN200A、200B、200CがRSVPをサポートしたルータ300A、300B、300Cを介して接続されている。インターネット100のルータ300もRSVPをサポートしている。そして、各2個のルータ300Aと300B間、300Bと300C間、300Cと300A間にそれぞれIPトンネル（図では101のみ示す）を設定し、LAN200Aと200B間のトラヒックは全てIPトンネル101を通し、LAN200Bと200C間のトラヒックは全て該当するIPトンネル（図示省略）を通し、LAN200Cと200A間のトラヒックも全て該当するIPトンネル（図示省略）を通すようにしてある。

【0031】このようなIPトンネル101の設定は、IPトンネル両端のマシン（IPトンネルサーバ）上にもIPトンネル機能を付加することにより行われる。つまり、IPトンネル一端のルータ例えば300Aが他端のルータ例えば300Bに対してIPトンネルの設定を要求することにより行われる。前述のように、IPトンネル始点（又は終点）によるIPパケットのカプセル化（又はカプセル解除）はRSVPによる帯域確保区間（図9の102参照）を含む範囲にて行われれば良いので、IPトンネル機能の付加は伝送帯域の提供者（例えば通信事業者）が行う場合も考えられ、また、図9

（b）に示すように伝送帯域のユーザがLAN200A、200B上にIPトンネルサーバ203で設定する場合もある。

【0032】なお、本実施例では、各2個のLAN200Aと200B間、200Bと200C間、200Cと200A間を、従来のVPNと同様、それぞれエンドー

エンドでのデータの暗号化、ユーザ認証及びアクセス制御等のセキュリティを施した上でインターネット100を介して接続している。

【0033】ルータ内部は、トラヒック制御のために、図2に示す構成としてある。一般に、ルータは入力側と出力側に複数のインターフェースを持つので、本実施例では、双方2つのインターフェースを持つものとして説明する。

【0034】そこで、ルータ内部には、データ伝送に先立つ網資源予約型プロトコル（RSVP）による帯域確保の過程において、入力側にはIPトンネル数（予約数）と同数N個のRSVP用入力バッファ301と、1個の非RSVP用（非予約型パケット用）入力バッファ302が作成される。また、出力側にはIPトンネル数（予約数）以上のL+M個のRSVP用出力バッファ303と、各出力インターフェース毎に1個の非RSVP用（非予約型パケット用）出力バッファ304が作成される。但し、各バッファ容量は各IPトンネルに予約した伝送帯域幅に応じて可変であるものとしている。

【0035】更に、ルータ内部には、入力用プロセッサ305及び各出力インターフェース毎の出力用プロセッサ306に加えて、予約識別用プロセッサ307と、これに連携する予約データベース308が設けられている。予約データベース308には、帯域予約の有無、各予約内容（送／受信側IPアドレス、Port（ポート）番号、プロトコルID、予約帯域幅等）の識別・照合・確認に必要なデータが格納される。図2中、311は元のパケット（IPデータグラム）309にIPトンネル両端のルータのIPアドレス等が記述されたIPヘッダ310を付加（カプセル化）したパケットを示す。

【0036】IPトンネルに伝送帯域幅を予約するには、基本的には、LAN上のホスト或いはサブネットが伝送帯域を必要とする時に、同ホスト或いはサブネットがRSVP帯域確保区間の一端のルータに伝送帯域確保の要求を通知し、また、IPトンネル上の送／受信側IPアドレス、ポート番号、プロトコルID、予約帯域幅等の予約内容を通知する。同ルータはRSVPによりこれらの通知を次々に途中のルータ及びIPトンネル他端のルータに転送する。各ルータは帯域予約とその内容を予約データベース308に格納する。いずれかのルータで帯域確保が不可能であれば、RSVPは帯域予約の要求を棄却する旨を始点のルータに通知する。

【0037】次に、図2及び図3、図4を参照して、ルータにおけるトラヒック制御を説明すると、下記（1）～（5）のようになる。

【0038】（1）図3のステップS1、S2のように、各入力インターフェースに到着したパケットに対し、予約識別用プロセッサ307がそれに連携する予約データベース308を参照して、帯域予約の有無、各予約内容（送／受信側IPアドレス、ポート番号、プロト

コル ID、予約帯域幅等)の識別・照合・確認を行う。

【0039】(2) これら帯域予約の有無と各予約内容の識別等の後、予約識別用プロセッサ 307 はバケットを各々予約した IP トンネルに対応する入力バッファへ割り振る(図 3 のステップ S 3)。

【0040】(3) 入力プロセッサ 305 はバケット配信処理の際に、優先度の高い入力バッファからバケットを取り出す(図 3 のステップ S 4)。具体的には、図 4 を例に説明すると、下記①②のようになる。

①今、図 4 に示すように、RSVP 用(帯域予約用)入力バッファ 301 が #1、#2、#3 の 3 個、非 RSVP 用(非予約型バケット用)入力バッファ 302 が 1 個有り、各 IP トンネルの予約帯域幅及び非予約型帯域幅の比が $i : j : k : x$ であるとする。

②入力プロセッサ 305 は各帯域幅比に応じた頻度 f 、で各入力バッファにアクセスして同バッファよりバケットを取り出す。具体的には、 $f_i = m / (i + j + k + x)$ で表される頻度である。但し、 m は i 、 j 、 k 、 x の何れかである。このようにして RSVP 用入力バッファ #1、#2、#3 をアクセスした時、取り出すべきバケットがなければ、非 RSVP 用入力バッファ 302 内のバケットを、若しそこにバケットがあれば取り出す。

【0041】(4) 上記入力バッファからのバケット取出処理の後、入力プロセッサ 305 は、バケットを対応する出力バッファへ送る(図 3 のステップ S 5)。

【0042】(5) その後、出力バッファ内のバケットを、各インターフェース毎に用意される出力プロセッサ 306 によって取り出し、ネットワークへ送出する(図 3 のステップ S 6 と S 7)。出力プロセッサ 306 が出力バッファ内のバケットを取り出す機能は、入力プロセッサ 305 を出力プロセッサ 306 と読み替え、入力バッファ #1 ~ #3 を出力バッファ #1 ~ #3 と読み替えるだけで上記(3)と同様であり、下記①②のようになる。

①今、図 4 に示すように、RSVP 用(帯域予約用)出力バッファ 303 が #1、#2、#3 の 3 個、非 RSVP 用(非予約型バケット用)入力バッファ 304 が 1 個有り、各 IP トンネルの予約帯域幅及び非予約型帯域幅の比が $i : j : k : x$ であるとする。

②出力プロセッサ 306 は各帯域幅比に応じた頻度 f 、で各出力バッファにアクセスして同バッファよりバケットを取り出す。具体的には、 $f_i = m / (i + j + k + x)$ で表される頻度である。但し、 m は i 、 j 、 k 、 x の何れかである。このようにして RSVP 用出力バッファ #1、#2、#3 をアクセスした時、取り出すべきバケットがなければ、非 RSVP 用出力バッファ 304 内のバケットを、若しそこにバケットがあれば取り出す。

【0043】次に、図 5 と図 6 を参照して、VPN の予約スケジュール機能を説明する。前述の如く、RSVP を用いた網資源予約では、本来、資源を必要とする時に

しか伝送帯域の予約ができないが、本実施例では、下記(I) ~ (V) の処理により、指定した日時での伝送帯域の予約を可能にしている。なお、図 5 のステップ S 28 は図 6 のステップ S 29 に続く。

【0044】(I) 帯域確保型 VPN 使用の事前予約が生じたら(図 5 のステップ S 21)、RSVP (網資源予約型プロトコル)により IP トンネル用の経路を設定可能かどうかを確認する(図 5 のステップ S 22)。設定不可能であれば、事前予約を棄却する(図 5 のステップ S 23、S 24)。

【0045】(II) 設定可能であれば、その IP トンネル用経路上の全ルータ内の予約データベース(図 2 の 308 参照)を参照して、当該日時に要求するだけの伝送帯域幅を確保可能かどうかを確認する(図 5 のステップ S 23、S 25)。確保不可能であれば、事前予約を棄却する(図 5 のステップ S 26、S 24)。

【0046】(III) 確保可能な場合は、IP トンネル用経路上の全ルータ内の予約データベースに必要な予約情報(日時、予約帯域幅、送/受信側 IP アドレス、ポート番号、プロトコル ID 等)を登録する(図 5 のステップ S 26、S 27)。

【0047】(IV) 指定日時になったら、下記①~②の処理をして、予約した伝送帯域幅の提供を開始する(図 5 のステップ S 28 ~ 図 6 のステップ S 31)。

①一定時間監視した後、予約者からのトラヒックが無いと判断される場合は、その事前予約を棄却する(図 5 のステップ S 28、S 24)。

②事前予約されていないトラヒック(スケジュール外トラヒック)による帯域不足が生じる場合は、そのスケジュール外トラヒックの種別により以下(a)(b)の処理でトラヒック抑制を行う(図 6 のステップ S 29、S 30)。

(a) スケジュール外トラヒックが非 RSVP プロトコル(非網資源予約型プロトコル)の場合は、同トラヒックを全て棄却する。

(b) スケジュール外トラヒックが RSVP プロトコルの場合は、その利用者に予約解除の旨のメッセージを送出し、予約を解除する。

【0048】(V) 指定日時が経過したら、予約した伝送帯域幅の提供を終了する(図 6 のステップ S 32)。

【0049】

【発明の効果】本発明によれば、インターネットに接続されるルータ間に IP トンネルを構成し、この IP トンネル上に網資源予約型プロトコルを起動させることにより同 IP トンネルの伝送帯域幅の予約を行うので、他のトラヒックの影響を避けることができ、従来の VPN よりも安定したトラヒック特性が得られる。また、網資源予約型プロトコルによる帯域確保がルータ間(IP トンネル)にて行われるので、アプリケーション毎の網資源の予約が不要になり、LAN 上の個々のホスト或いはサ

ブネットは網資源予約型プロトコルをサポートしなくても良い。更に、帯域確保は網資源予約型プロトコルにより行われるので、帯域確保の設定及び解除が容易である。従って、各ノードのパラメータを手作業で変更する必要がなく、人的コストが削減できる。また、短期的な帯域需要に対して迅速且つ柔軟に伝送帯域幅を割り当てることができ、短期間の利用で大容量のデータ伝送が必要とされる場合に極めて有効である。

【0050】また、本発明によれば、IPトンネル上のルータのトラヒック制御として、同ルータ内部の入出力プロセッサ及び出力プロセッサが処理するパケット送出頻度を、各IPトンネルに予約した伝送帯域幅の比で割り当てることにより、トラヒック制御のアルゴリズムが極めて簡素化する。

【0051】更に、本発明によれば、IPトンネル上の各ルータに予約スケジュール機能を持たせ、帯域確保型VPNの使用時間の管理を行うことにより、網資源予約型プロトコルを用いた予約では本来網資源を必要とする時にしか予約できないものが、将来の指定した日時での伝送帯域幅を確保することができる。

【図面の簡単な説明】

【図1】本発明を適用したネットワークモデルを示す図。

【図2】ルータ内部のトラヒック制御の構成例を示す図。

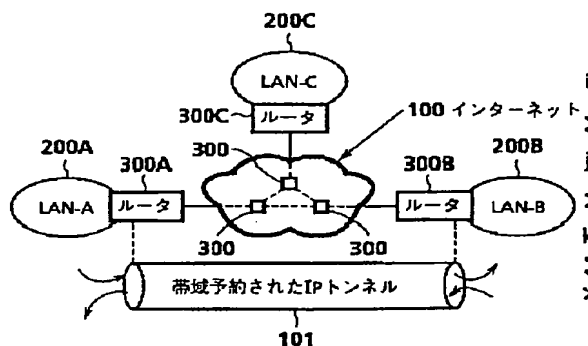
【図3】図2の構成におけるトラヒック制御手順を示す図。

【図4】トラヒック制御におけるパケットキューイングの説明図。

【図5】ルータにおけるVPN予約スケジュールの処理手順（その1）を示す図。

【図1】

ネットワークモデル (実施例)



【図6】ルータにおけるVPN予約スケジュールの処理手順（その2）を示す図。

【図7】従来のRSVPを示す図。

【図8】LANのホストがRSVPをサポートしない場合の従来のRSVPの欠点を示す図。

【図9】本発明の原理を示す図。

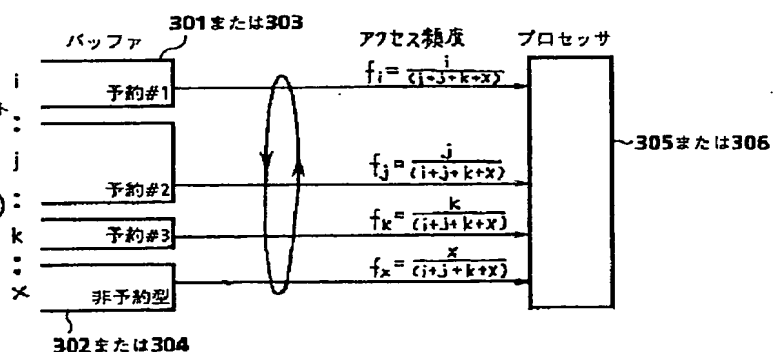
【図10】パケットスケジューリングのアルゴリズム簡素化の説明図。

【符号の説明】

100	インターネット
101	IPトンネル
102	RSVPによる帯域確保区間
200A、200B、200C	LAN
201	ホスト
202	アプリケーション
203	IPトンネルサーバ
300A、300B、300C、300	ルータ
301	RSVP用入力バッファ
302	非RSVP用入力バッファ
303	RSVP用出力バッファ
304	非RSVP用出力バッファ
305	入力プロセッサ
306	出力プロセッサ
307	予約識別用プロセッサ
308	予約データベース
309	IPデータグラム
310	IPヘッダ
401	パケットスケジューラ
402	RSVP用（IPトンネル用）バッファ
403	非RSVP用バッファ

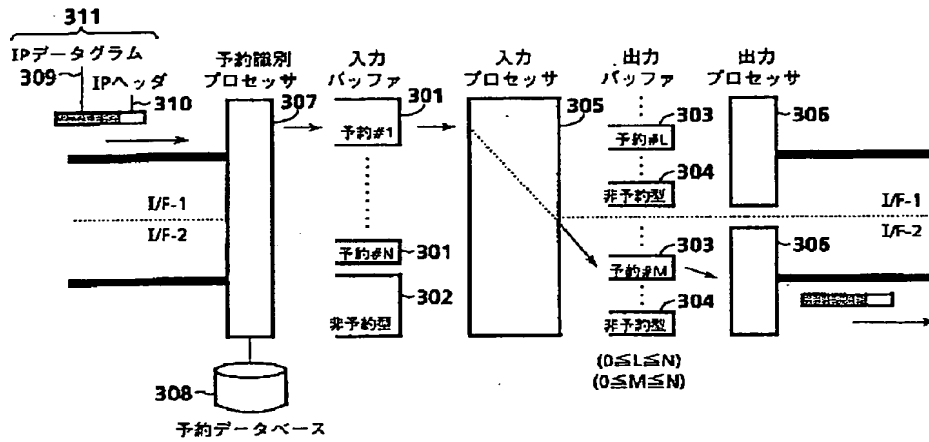
【図4】

パケットキューイング



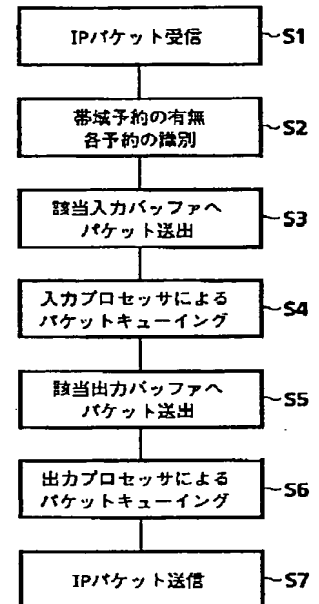
【図 2】

ルータでのトラヒック制御



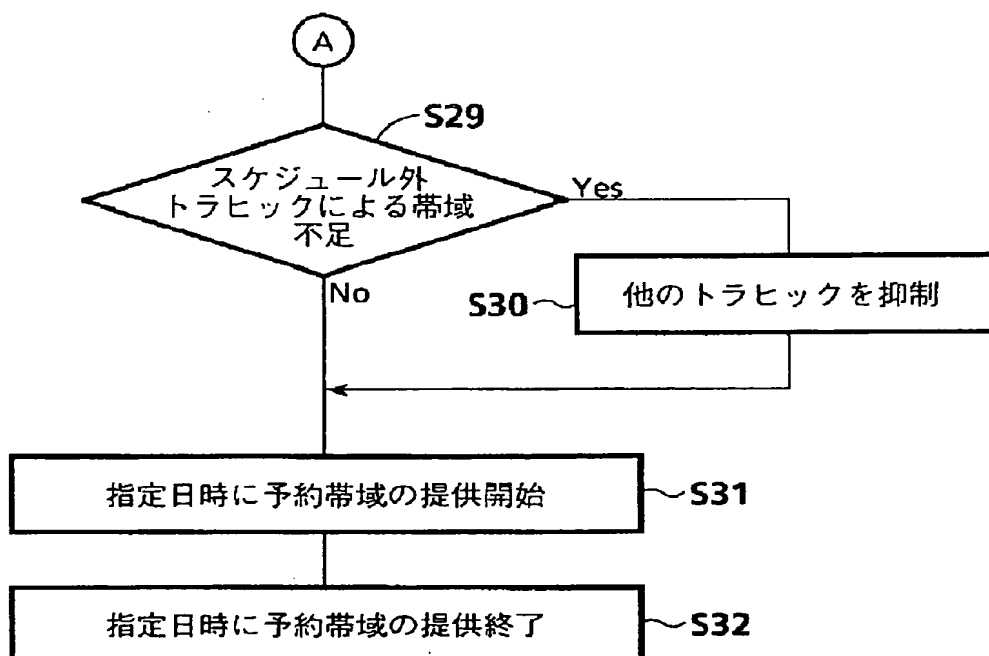
【図 3】

実施例 (ルータにおけるトラヒック制御)



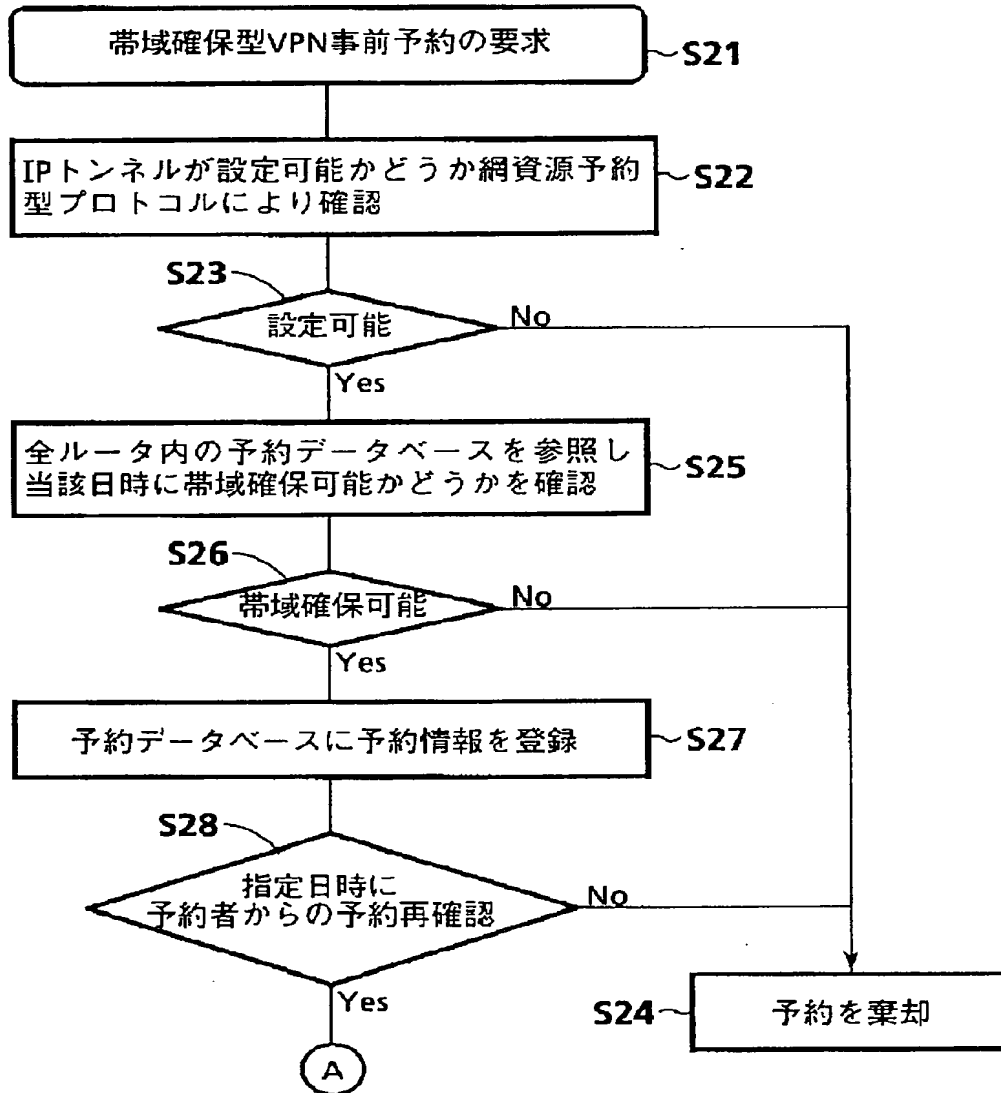
【図 6】

VPNの予約スケジュール機能 (その2)



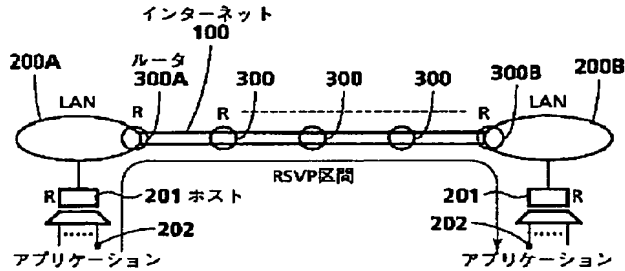
【図 5】

VPNの予約スケジュール機能(その1)



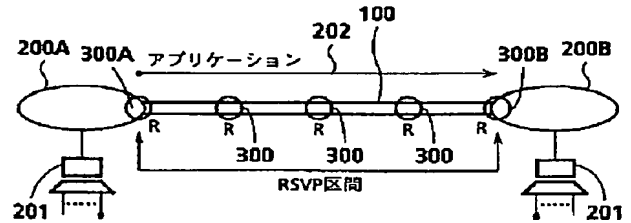
【 図 7 】

従来の RSVP



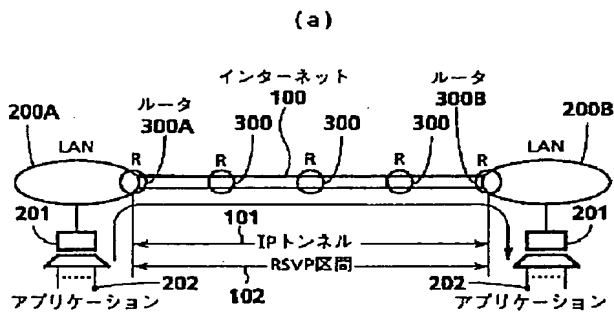
【 図 8 】

従 来



【 図 9 】

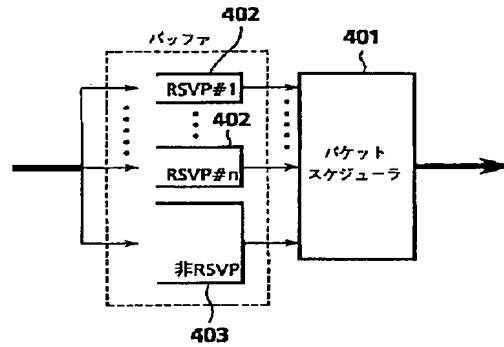
発 明 (原 理)



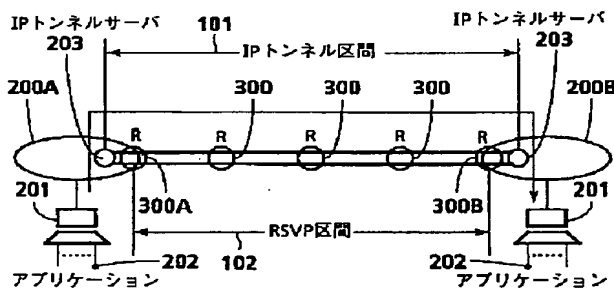
(a)

【 図 1 0 】

発 明 (パ ケ ッ ト ス ケ ジ ュ ー リ ン グ)



(b)



フロントページの続き

(72)発明者 浅見 徹
 東京都新宿区西新宿二丁目 3 番 2 号 国際
 電信電話株式会社内